Electronic Version

Stylesheet Version v1.1.1

Claims

[c1] A method of secure distribution of encryption/decryption keys among two communicating parties comprising of:

public (non-secret) selecting a natural number n;

public (non-secret) selecting a natural number k;

public (non-secret) selecting a k-tuple $S = (S_1, S_2, \ldots, S_k)$ of pairwise-commuting $n \times n$ matrices with integer coefficients;

private (non-public) generating the polynomial $p(x_1, x_2, \ldots, x_k)$ in k variables $x_1, x_2, \ldots, x_k$ and with integer coefficients by the first communicating party;

private (non-public) generating the polynomial $q(x_1, x_2, \ldots, x_k)$ in k variables $x_1, x_2, \ldots, x_k$ and with integer coefficients by the second communicating party;

private (non-public) generating $n \times n$ matrix A with integer coefficients by the first communicating party according to the formula:

$A = p(S_1, S_2, \ldots, S_k)$;

private (non-public) generating $n \times n$ matrix B with integer coefficients by the second communicating party:

$B = q(S_1, S_2, \ldots, S_k)$,

(therefore, $A \cdot B = B \cdot A$);

public (non-secret) selecting a compact topological monoid G by both communicating parties;
public (non-secret) selecting an n-tuple $g = (g_1, g_2,\ldots,g_n)$ of pairwise commuting elements in G by both communicating parties;
generating the n-tuple g^A by the first communicating party by the formula:
$g^A=(y_1, y_2,\ldots,y_n)$,
where
$y_j=g_1^{A1,j}\cdot g_2^{A2,j}\cdot\ldots\cdot g_n^{An,j}$
for j = 1, 2, ..., n, where each A_{ij} is a corresponding matrix coefficient of the matrix A;
generating the n-tuple g^B by the second communicating party by the formula:
$g^B=(z_1, z_2,\ldots, z_n)$,
where
$z_j=g_1^{B1,j}\cdot g_2^{B2,j}\cdot\ldots\cdot g_n^{Bn,j}$
for j = 1, 2, ..., n, where each B_{ij} is a corresponding matrix coefficient of the matrix B;
public (non-secret) transmitting the n-tuple g^A from the first communicating party to the second communicating party;
public (non-secret) transmitting the n-tuple g^B from the second communicating party to the first communicating party;
creating the shared secrete key $g^{A\cdot B}$ by the communi-

cating parties: generating the n–tuple $(g^A)^B$ by the second communicating party and generating the n–tuple $(g^B)^A$ by the first communicating party (since $(g^A)^B = g^{A \cdot B} = g^{B \cdot A} = (g^B)^A$, both communicating parties possess this n–tuple $g^{A \cdot B}$).

[c2] The method as defined by claim 1, wherein G is an arbitrary compact topological monoid and the polynomials $p(x_1, x_2, \ldots, x_k)$ and $q(x_1, x_2, \ldots, x_k)$ have non–negative integer coefficients, and all the matrices $S_1, S_2, \ldots, S_k$ have non–negative integer matrix coefficients.

[c3] The method as defined by claim 1, wherein G is an arbitrary compact topological group and the polynomials $p(x_1, x_2, \ldots, x_k)$ and $q(x_1, x_2, \ldots, x_k)$ have arbitrary integer coefficients, and all the matrices $S_1, S_2, \ldots, S_k$ have arbitrary integer matrix coefficients.

[c4] The method as defined by claims 1 and 2, wherein G is an arbitrary compact topological monoid, $k = 1$ and the $n \times n$ matrix S has non–negative integer matrix coefficients so that

$A = a_0 \cdot I + a_1 \cdot S + a_2 \cdot S^2 + \ldots + a_{n-1} \cdot S^{n-1}$ and $B = b_0 \cdot I + b_1 \cdot S + b_2 \cdot S^2 + \ldots + b_{n-1} \cdot S^{n-1}$,

where $a_0, a_1, \ldots, a_{n-1}$ are non–negative integers privately generated by the first communicating party and $b_0, b_1, \ldots, b_{n-1}$ are non–negative integers privately gen–

erated by the second communicating party, and where I is the identity $n \times n$ matrix.

[c5] The method as defined by claims 1 and 3, wherein G is an arbitrary compact topological group, $k = 1$ and the $n \times n$ matrix S has arbitrary integer matrix coefficients so that

$A = a_0 \cdot I + a_1 \cdot S + a_2 \cdot S^2 + \ldots + a_{n-1} \cdot S^{n-1}$ and $B = b_0 \cdot I + b_1 \cdot S + b_2 \cdot S^2 + \ldots + b_{n-1} \cdot S^{n-1}$,

where $a_0, a_1, \ldots, a_{n-1}$ are arbitrary integers privately generated by the first communicating party and $b_0, b_1, \ldots, b_{n-1}$ are arbitrary integers privately generated by the second communicating party, and where I is the identity $n \times n$ matrix.

[c6] The method as defined by claims 1, 2, and 4, wherein G is an arbitrary compact topological monoid, $k = 1$, $n = 2$, and the 2×2 matrix S has non-negative integer matrix coefficients $s_{11}, s_{12}, s_{21}, s_{22}$ so that

$$A = \begin{bmatrix} a_0 + a_1 s_{11} & a_1 s_{12} \\ a_1 s_{21} & a_0 + a_1 s_{22} \end{bmatrix}$$

and

$$B = \begin{bmatrix} b_0 + b_1 s_{11} & b_1 s_{12} \\ b_1 s_{21} & b_0 + b_1 s_{22} \end{bmatrix}$$

where a_0, a_1 are non-negative integers privately generated by the first communicating party and b_0, b_1 are non-negative integers privately generated by the second communicating party. Therefore,

$$A \cdot B = B \cdot A = \begin{bmatrix} a_0b_0+(a_0b_1+b_0a_1+a_1b_1s_{11})s_{11}+a_1b_1s_{12}s_{21} & (a_0b_1+b_0a_1+a_1b_1s_{11}+a_1b_1s_{22})s_{12} \\ (a_0b_1+b_0a_1+a_1b_1s_{11}+a_1b_1s_{22})s_{21} & a_0b_0+(a_0b_1+b_0a_1+a_1b_1s_{22})s_{22}+a_1b_1s_{12}s_{21} \end{bmatrix}$$

[c7] The method as defined by claims 1, 3, and 5, wherein G is an arbitrary compact topological group, $k = 1$, $n = 2$, and the 2×2 matrix S has arbitrary integer matrix coefficients s_{11}, s_{12}, s_{21}, s_{22} so that

$$A = \begin{bmatrix} a_0 + a_1 s_{11} & a_1 s_{12} \\ a_1 s_{21} & a_0 + a_1 s_{22} \end{bmatrix}$$

and

$$B = \begin{bmatrix} b_0 + b_1 s_{11} & b_1 s_{12} \\ b_1 s_{21} & b_0 + b_1 s_{22} \end{bmatrix}$$

where a_0, a_1 are arbitrary integers privately generated by the first communicating party and b_0, b_1 are arbitrary integers privately generated by the second communicating party. Therefore,

$$A \cdot B = B \cdot A = \begin{bmatrix} a_0b_0+(a_0b_1+b_0a_1+a_1b_1s_{11})s_{11}+a_1b_1s_{12}s_{21} & (a_0b_1+b_0a_1+a_1b_1s_{11}+a_1b_1s_{22})s_{12} \\ (a_0b_1+b_0a_1+a_1b_1s_{11}+a_1b_1s_{22})s_{21} & a_0b_0+(a_0b_1+b_0a_1+a_1b_1s_{22})s_{22}+a_1b_1s_{12}s_{21} \end{bmatrix}$$

[c8] The method as defined by claims 1 and 2, wherein G is an arbitrary compact topological monoid, $k = 2$ and the $n \times n$ matrices S_1 and S_2 have non-negative integer matrix coefficients and satisfy $S_1 \cdot S_2 = S_2 \cdot S_1$ so that $A = \Sigma^{n-1}_{i,j=0}\, a_{i,j} \cdot S_1^{\,i} \cdot S_2^{\,j}$ and $B = \Sigma^{n-1}_{i,j=0}\, b_{i,j} \cdot S_1^{\,i} \cdot S_2^{\,j}$, where all $a_{i,j}$, i = 0, 1, ..., n−1, and j = 0, 1, ..., n−1, are non-negative integers privately generated by the first communicating party and all $b_{i,j}$, i = 0, 1, ..., n−1, and j = 0, 1, ..., n−1, are non-negative integers privately generated by the second communicating party, and where I is the identity $n \times n$ matrix.

[c9] The method as defined by claims 1 and 3, wherein G is an arbitrary compact topological group, $k = 2$ and the $n \times n$ matrices S_1 and S_2 have arbitrary integer matrix coefficients and satisfy $S_1 \cdot S_2 = S_2 \cdot S_1$ so that $A = \Sigma^{n-1}_{i,j=0}\, a_{i,j} \cdot S_1^{\,i} \cdot S_2^{\,j}$ and $B = \Sigma^{n-1}_{i,j=0}\, b_{i,j} \cdot S_1^{\,i} \cdot S_2^{\,j}$,

where all $a_{i,j}$, i = 0, 1, …, n−1, and j = 0, 1, …, n−1, are arbitrary integers privately generated by the first communicating party and all $b_{i,j}$, i = 0, 1, …, n−1, and j = 0, 1, …, n−1, are arbitrary integers privately generated by the second communicating party, and where I is the identity $n \times n$ matrix.

[c10] The method as defined by claim 1, wherein n = 1 and G is any compact topological monoid and the said 1×1 matrices A and B are any non-negative integers.

[c11] The method as defined by claim 1, wherein n = 1 and G is any compact topological group and the said 1×1 matrices A and B are arbitrary integers.

[c12] The method as defined by claims 1, 2, 4, 6, and 8 wherein G is any commutative compact topological monoid.

[c13] The method as defined by claims 1, 3, 5, 7, and 9, wherein G is any commutative compact topological group.

[c14] The method as defined by claim 11, wherein n = 1 and G is any connected compact Lie group.

[c15] The method as defined by claim 11, wherein n = 1 and said G is a connected closed subgroup of the orthogonal

group O(V), where V is a Euclidean vector space.

[c16] The method as defined by claim 11, wherein $n = 1$ and said G is a connected closed subgroup of the unitary group U(W), where W is a Hermitian vector space.

[c17] The method as defined by claim 15, wherein the group G is the special orthogonal group SO(V), that is, G is the connected component of the identity in the orthogonal group O(V).

[c18] The method as defined by claim 16, wherein the group G is the unitary group U(W).

[c19] The method as defined by claim 15, wherein the set V is a Euclidean vector space of dimension m, where m is an integer greater than 1.

[c20] The method as defined by claim 16, wherein the set W is a Hermitian vector space of dimension m, where m is an integer greater than 0.

[c21] The method as defined by claim 19, wherein said V is the real vector space R^m with the standard Euclidean dot product:

$$x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_m y_m$$

for any vectors $x = [x_1, x_2, \ldots, x_m]$ and $y = [y_1, y_2, \ldots, y_m]$ of R^m.

[c22] The method as defined by claim 16, wherein said W is the complex vector space C^n with the standard Hermitian dot product:

$x \cdot y^* = x_1 y_1^* + x_2 y_2^* + \ldots + x_m y_m^*$

for any vectors $x = [x_1, x_2, \ldots, x_m]$ and $y = [y_1, y_2, \ldots, y_m]$ of C^m, where y_i^* is the complex conjugate number of the complex number y_i.

[c23] The method as defined by claims 17 and 21, wherein the group G is the group SO_m of special orthogonal $m \times m$ matrices, that is, SO_m is the set of all real $m \times m$ matrices M such that the determinant of M is 1 and $M \cdot M^T = I$, where M^T is the transposed matrix of M and Iis the identity $m \times m$ matrix.

[c24] The method as defined by claims 18 and 22, wherein the group G is the group U_m of unitary$m \times m$ matrices, that is, U_m is the set of all complex $m \times m$ matrices M such that $M \cdot M^* = I$, where M^* is the transposed complex conjugate matrix of M and I is the identity $m \times m$ matrix.

[c25] The method as defined by claims 23 and 24, wherein the group G is any of two isomorphic groups SO_2 or U_1.

[c26] The method as defined by claims 13 and 25, wherein the group G is a torus of dimension m, that is, G is direct product of m copies of the group U_1.

[c27] The method of claim 25, wherein as the group G is further defined as the semi-open interval [0, 1) of real numbers that includes 0 but does not include 1, where the group operation "*" is the fractional part of the sum:

g*h = {g+ y}

for any real g and h in the semi-open interval [0, 1), where $\{z\}$ stands for the fractional part of a real number z.

[c28] The method as defined by the claims 1 and 27, wherein the said n-tuple g is given by:

$g = (g_1, g_2, \ldots, g_n)$,

where $g_1, g_2, \ldots, g_n$ are real numbers in the semi-open interval [0,1); and for a given integer $n \times n$ matrix $A = (A_{ij})$ the power g^A is given by:

$g^A = (y_1, y_2, \ldots, y_n)$,

where $y_j = \{g_1 A_{1,j} + g_2 A_{2,j} + \ldots + g_n A_{n,j}\}$ for j = 1, 2, ..., n; and for a given integer $n \times n$ matrix $B = (B_{ij})$ the power g^B is given by:

$g^B = (z_1, z_2, \ldots, z_n)$,

where $z_j = \{g_1 B_{1,j} + g_2 B_{2,j} + \ldots + g_n B_{n,j}\}$ for j = 1, 2, ..., n.

[c29] The method as defined by the claims 1, 7, 27, and 28, wherein $n = 2$, $g = (g_1, g_2)$, the 2×2 matrices A and B are given by:

$$A = \begin{bmatrix} a_0 + a_1 s_{11} & a_1 s_{12} \\ a_1 s_{21} & a_0 + a_1 s_{22} \end{bmatrix}$$

and

$$B = \begin{bmatrix} b_0 + b_1 s_{11} & b_1 s_{12} \\ b_1 s_{21} & b_0 + b_1 s_{22} \end{bmatrix}$$

and the powers g^A and g^B are given by:

$g^A = (y_1, y_2)$,

where

$y_1 = \{g_1(a_0 + a_1 s_{11}) + g_2(a_1 s_{21})\}$ and $y_2 = \{g_1(a_1 s_{12}) + g_2(a_0 + a_1 s_{22})\}$;

and

$g^B = (z_1, z_2)$,

where

$z_1 = \{g_1(b_0 + b_1 s_{11}) + g_2(b_1 s_{21})\}$ and $z_2 = \{g_1(b_1 s_{12}) + g_2(b_0 + b_1 s_{22})\}$;

Therefore, the shared key $g^{A \bullet B} = g^{B \bullet A} = (k_1, k_2)$ is given by:

$k_1 = \{(a_0 b_0 + (a_0 b_1 + b_0 a_1 + a_1 b_1 s_{11}) s_{11} + a_1 b_1 s_{12} s_{21}) g_1 + (a_0 b_1 + b_0 a_1 + a_1 b_1 s_{11} + a_1 b_1 s_{22}) s_{21} g_2\}$,

$k_2 = \{(a_0 b_1 + b_0 a_1 + a_1 b_1 s_{11} + a_1 b_1 s_{22}) s_{12} g_1 + (a_0 b_0 + (a_0 b_1 + b$

$a_1+a_1b_1s_{22})s_{22}+a_1b_1s_{12}s_{21})g_2\}$

[c30] Method as defined by the claims 1, 7, 27, 28, and 29, wherein $n = 2$, $g = (g_1, g_2)$, and the said matrix S is given by

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

therefore:

the 2×2 matrices A and B are given by:

$$A = \begin{bmatrix} a_0 & -a_1 \\ a_1 & a_0 \end{bmatrix}$$

and

$$B = \begin{bmatrix} b_0 & -b_1 \\ & \\ b_1 & b_0 \end{bmatrix}$$

the powers g^A and g^B are given by:

$g^A = (y_1, y_2)$,

where

$y_1 = \{g_1 a_0 + g_2 a_1\}$ and $y_2 = \{-g_1 a_1 + g_2 a_0\}$; and

$g^B = (z_1, z_2)$,

where

$z_1 = \{g_1 b_0 + g_2 b_1\}$ and $z_2 = \{-g_1 b_1 + g_2 b_0\}$;

Therefore, the shared key $g^{A \cdot B} = g^{B \cdot A} = (k_1, k_2)$ is given by:

$k_1 = \{(a_0 b_0 - a_1 b_1) g_1 + (a_0 b_1 + b_0 a_1) g_2\}$,

$k_2 = \{-(a_0 b_1 + b_0 a_1) g_1 + (a_0 b_0 - a_1 b_1) g_2\}$.

[c31] The method as defined by the claim 27, wherein for each natural number P, each element g of the group G is rounded to a rational element $[g]_P$ of the group G according to the formula: $[g]_P = (\mathrm{Round}(gP))/P$

if Round(gP)<P, and

$[g]_P = 0$

if Round(gP)=P, where Round(z) stands for the standard

rounding of a real number z to the closest integer.

[c32] The method as defined by the claims 27 and 31, wherein for each n-tuple $P=(P_1, P_2,..., P_n)$ of natural numbers, each n-tuple $g=(g_1, g_2,..., g_n)$ of elements of the group G is rounded to a rational n-tuple $[g]_P$ according to the formula:

$[g]_P=([g_1]_{P\,1}, [g_2]_{P\,2}, ..., [g_n]_{P\,n})$.

[c33] A method of secure distribution of encryption/decryption keys among two communicating parties comprising of:

public (non-secret) selecting a natural number n and k as in claim 1;

public (non-secret) selecting a k-tuple $S = (S_1, S_2,..., S_k)$ of pairwise-commuting $n\times n$ matrices with integer coefficients as in claim 1;

public (non-secret) selecting n-tuples natural numbers $P=(P_1, P_2,..., P_n)$,$Q=(Q_1, Q_2,..., Q_n)$, and $K=(K_1, K_2,..., K_n)$;

public (non-secret) selecting a natural number D>1;

public (non-secret) selecting the commutative compact topological group G as in claim 27;

public (non-secret) selecting an n-tuple $g = (g_1, g_2,...,g_n)$ elements in G as in claims 28, 29, 30, 31 and 32;

private (non-public) generating the polynomial $p(x_1, x_2, ..., x_k)$ in k variables $x_1, x_2, ..., x_k$ and with integer coefficients by the first communicating party as in claim 1;

private (non-public) generating the polynomial $q(x_1, x_2, \ldots, x_k)$ in k variables $x_1, x_2, \ldots, x_k$ and with integer coefficients by the second communicating party as in claim 1;
private (non-public) generating $n\times n$ matrix A with integer coefficients by the first communicating party as in claim1;
private (non-public) generating $n\times n$ matrix B with integer coefficients by the first communicating party as in claim1;
generating the n-tuple g^{A} by the first communicating party as in claim 1;
generating the P-rounded n-tuple $[g^{A}]_P$ by the first communicating party as in claim 32;generating the n-tuple g^{B} by the second communicating party as in claim 1;
generating the Q-rounded n-tuple $[g^{B}]_Q$ by the second communicating party as in claim 32;
public (non-secret) transmitting the n-tuple $[g^{A}]_P$ from the first communicating party to the second communicating party;
public (non-secret) transmitting the n-tuple $[g^{B}]_Q$ from the second communicating party to the first communicating party;
creating the shared secrete key by the communicating parties: generating the n-tuple $[([g^{A}]_P)^{B}]_K$ by the second communicating party and generating the n-tuple $[([g^{B}]_Q)$

$]_K$ by the first communicating party.

[c34] The method as defined by the claims 28, 29, 30, 31, 32, and 33, wherein at least one coordinate of the said vector $g=(g_1, g_2,\ldots, g_n)$ is an irrational number.

[c35] The method as defined by the claims 28, 29, 30, 31, 32, and 33, wherein each coordinate g_i of the said vector $g=(g_1, g_2,\ldots, g_n)$ is a rational number of the form

$g_i=M_i/N_i$,

where $0\leq M_i < N_i$.

[c36] The method as defined by the claim 33, wherein the n-tuples of natural numbers $P=(P_1, P_2,\ldots, P_n)$,$Q=(Q_1, Q_2,\ldots, Q_n)$, and $K=(K_1, K_2,\ldots, K_n)$ and the natural number D satisfy the following compatibility conditions:

$Q^{-1}\cdot\alpha\leq (D\cdot K)^{-1}$, $P^{-1}\cdot\beta\leq (D\cdot K)^{-1}$,

where α and β are arbitrary public (non-secret) $n\times n$ matrices with natural coefficients α_{ij} and β_{ij} respectively such that:

$| A_{ij}|<\alpha_{ij}$, $| B_{ij}|<\beta_{ij}$

for all $i=1,2,.., n$, $j=1,2,..,n$; and $P^{-1}= (1/P_1,1/P_2,\ldots,1/P_n)$, $Q^{-1}= (1/Q_1,1/Q_2,\ldots,1/Q_n)$, $(D\cdot K)^{-1}= (1/(DK_1),1/(DK_2),\ldots,1/(DK_n))$, and the vector inequality

$(y_1, y_2, \ldots, y_n) \leq (z_1, z_2, \ldots, z_n)$

is equivalent to n scalar inequalities:

$y_1\leq z_1$, $y_2\leq z_2$, …, $y_n\leq z_n$. The compatibility conditions

guarantee that either at least one coordinate of $[([g^A]_P)^B]_{D \cdot K}$ equals 0, or at least one coordinate of $[([g^B]_Q)^A]_{D \cdot K}$ equals 0, or

$([g^A]_P)^B - ([g^B]_Q)^A = \theta \cdot (D \cdot K)^{-1}$,

where $-½ < \theta < ½$.

[c37] The method as defined by the claim 33, wherein a vector $x=(x_1, x_2, \ldots, x_n)$ is defined to be (K, D)-consistent if:

$(-c, -c, \ldots, -c) \le x-[x]_K \le (c, c, \ldots, c)$,

where $c=1/2-1/(2D)$.

[c38] The method as defined by the claims 33, 36, and 37 wherein both n-tuples $([g^A]_P)^B$ and $([g^B]_Q)^A$ are (K, D)-consistent, which guarantees the equality of the shared keys:

$[([g^A]_P)^B]_K = [([g^B]_Q)^A]_K$.

[c39] The method as defined by the claims 30, 33, 35, 36, and 37, wherein

$g=(M_1/N_1, M_2/N_2)$,

where $0 \le M_1 < N_1$, $0 \le M_1 < N_2$; and the 2×2 matrices A and B are given by:

$$A = \begin{bmatrix} a_0 & -a_1 \\ a_1 & a_0 \end{bmatrix}$$

and

$$B = \begin{bmatrix} b_0 & -b_1 \\ b_1 & b_0 \end{bmatrix}$$

where $|a_0|<\alpha_0$, $|a_1|<\alpha_1$, $|b_0|<\beta_0$, $|b_1|<\beta_1$, where α_0, α_1, β_0, β_1 are natural numbers each of which does not exceed $N_1 \cdot N_2$; and:

$\alpha_0/Q_1+\alpha_1/Q_2 \le 1/(DK_1)$, $\alpha_1/Q_1+\alpha_0/Q_2 \le (1/DK_2)$,

$\beta_0/P_1+\beta_1/P_2 \le 1/(DK_1)$, $\beta_1/P_1+\alpha_0/P_2 \le 1/(DK_2)$.

[c40] The method as defined by the claims 36, 37, 38, and 39, wherein each coordinate K_i of the said n-tuple $K=(K_1, K_2, \ldots, K_n)$ is given by the formula:

$K_i = r^{C_i^n}$

for i=1,2, …, n, where r is a natural number, and C1, C2, …, Cn are non-negative integers.

[c41] The method as defined by the claims 36, 37, 38, 39, and 40, wherein each i-th coordinate of the shared key $[([g^{A}]_{P})^{B}]_{K} = [([g^{B}]_{Q})^{A}]_{K}$ is presented as a rational r-ary number having at most Ci r-ary digits after the dot.